NetClarity
NACwall

RSA SecurID Ready Implementation Guide

Last Modified: November 22, 2011

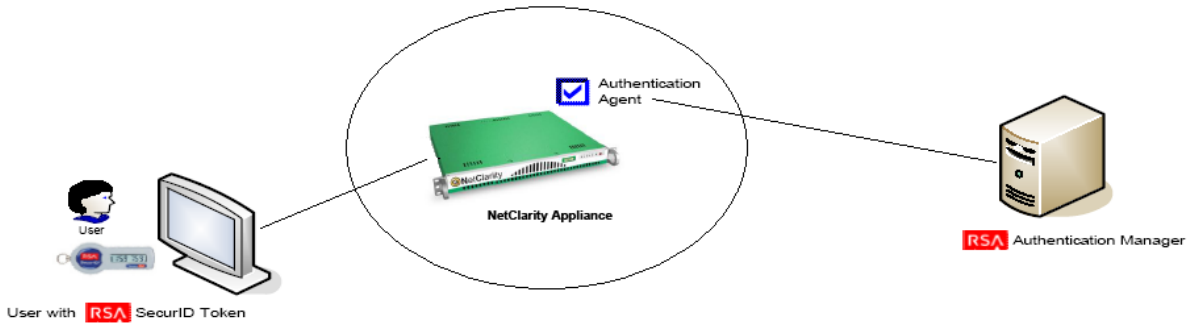
Partner Information

Product Information	
Partner Name	NetClarity
Web Site	www.netclarity.net
Product Name	NetClarity NACwall
Version & Platform	8.0.20
Product Description	NetClarity's NACwall appliances are designed to harden your network and provide immediate threat assessment and remediation capabilities.

Solution Summary

NetClarity's NACwall appliances are designed to harden your network and provide immediate threat assessment and remediation capabilities. This ensures compliance to the most stringent regulatory guidelines while thwarting malicious attempts to gain access to your network data. NACwall appliances can increase the quality of your audit and compliance reporting and decrease the time, effort and expense in doing so. They provide real-time internal network access control with e-mail, cell-phone paging, syslog and snmp traps reporting and logging capabilities. The NetClarity NACwall utilizes RSA SecurID to offer end users an added layer of security when logging into and managing the NACwall appliance. Appliance managers must posses a valid RSA Token to be able to authenticate with the NACwall appliance and gain access to the appliance management console. Appliance managers must also have a valid appliance or Active Directory account. Utilizing RSA SecurID ensures that no unauthorized access to the appliance is granted.

RSA SecurID supported features	
NetClarity NACwall 8.0.20	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
On-Demand Authentication via API	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with the NetClarity NACwall will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	/var/ace
Node Secret	/var/ace
sdstatus.12	/var/ace
sdopts.rec	/var/ace

Note: The appendix of this document contains more detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the NetClarity NACwall with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

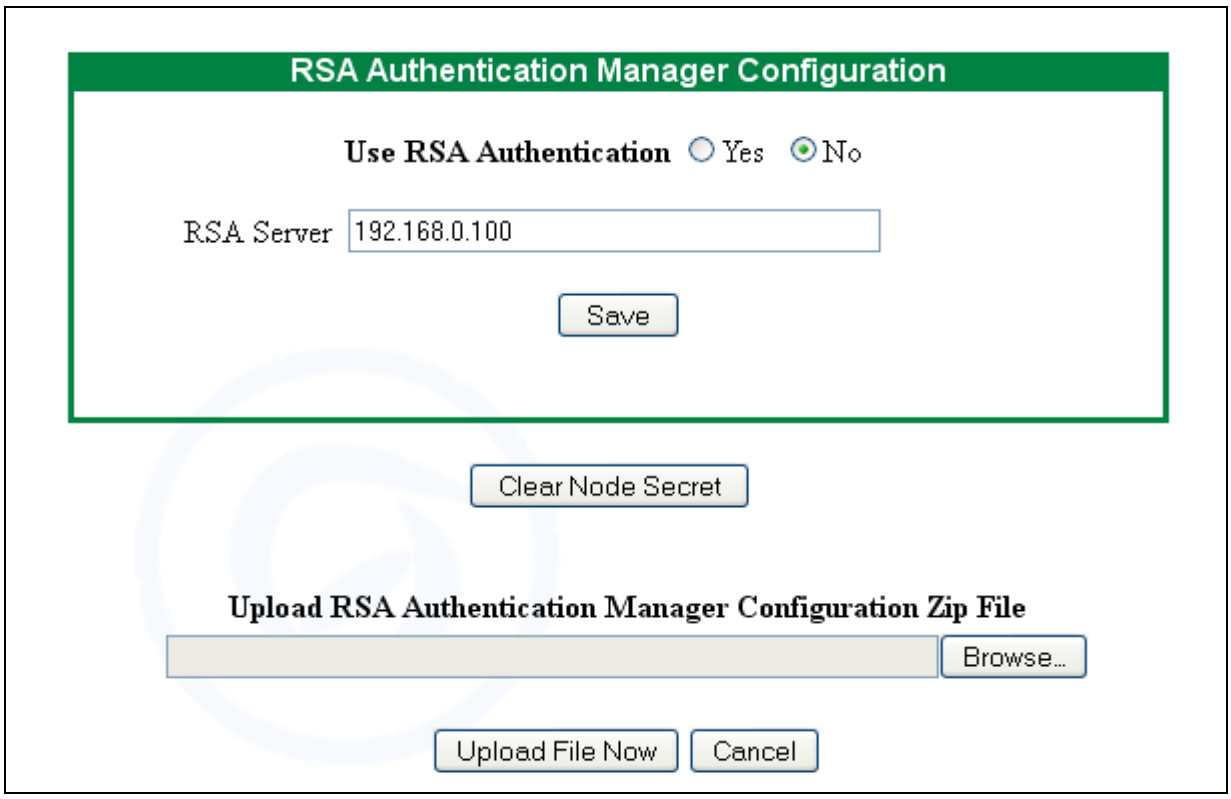
All NetClarity NACwall components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring RSA SecurID support in the NetClarity NACwall

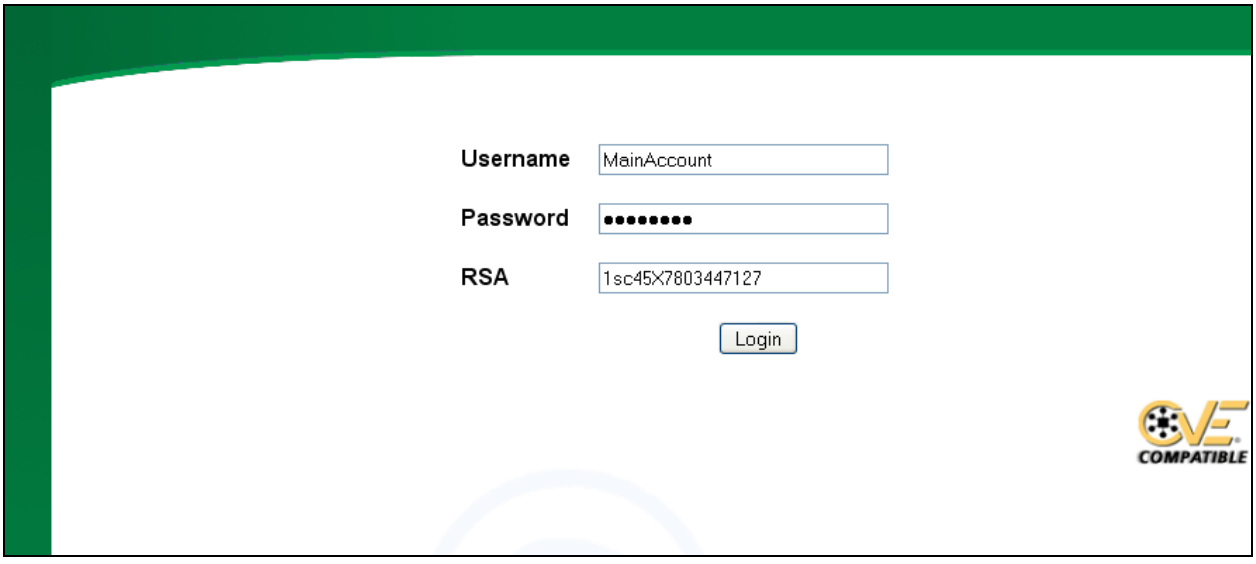
1. Logon to the NACwall and select **System > RSA Configuration**.
2. Select **Yes - Use RSA Authentication**.
3. Enter RSA Authentication Manager Server IP or hostname.
4. Click **Save**.
5. Click **Browse** to select your RSA Authentication Manager Configuration Zip File
6. Click **Upload File Now**.

Screens

Login screen:

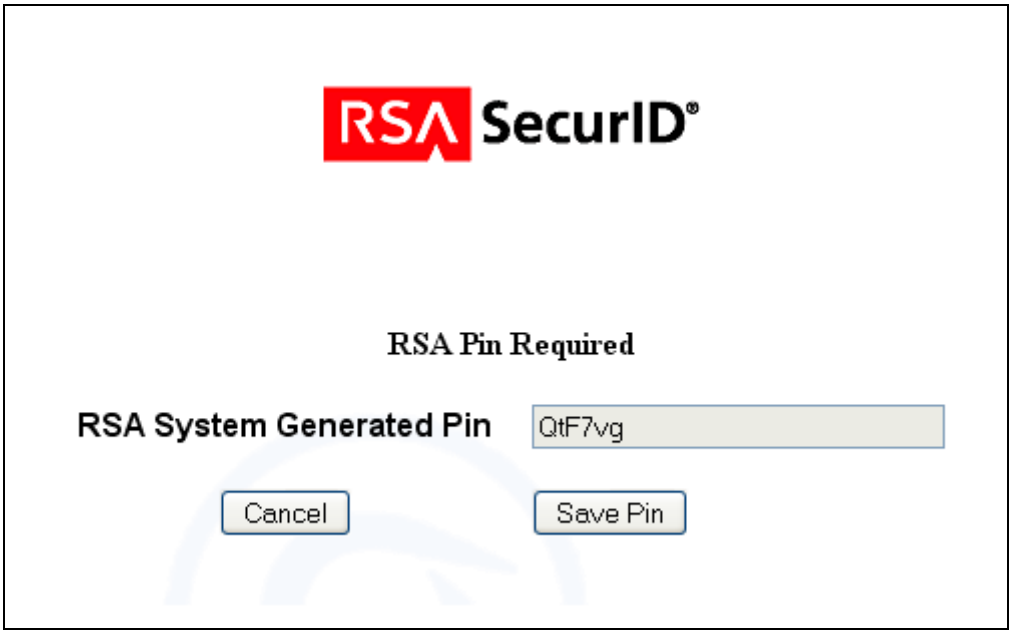


After enabling RSA Authentication NetClarity NACwall users are required to utilize their RSA credentials in addition to their NACwall, or active directory, credentials.



User-generated New PIN:

System-generated New PIN:



Next Tokencode:

Certification Checklist for RSA Authentication Manager

Date Tested: November, 22, 2011

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1SP4	Windows Server 2003 Enterprise
RSA Authentication Agent	1.40	Linux
NetClarity NACwall	8.0.20	Linux

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	✓	Deny Numeric PIN	N/A
Deny PIN Reuse	✓	Deny PIN Reuse	N/A
Passcode			
16-Digit Passcode	✓	16-Digit Passcode	N/A
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	N/A
On-Demand New PIN	✓	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

GLS / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Appendix

Partner Integration Details	
RSA SecurID API	v8.1.0.236.04_12_10_06_52_08
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users, Default Method
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

The Node Secret is shared between the RSA Authentication manager and the agent stored in the NetClarity NACwall. The Node Secret will be created and stored by the system. No action is required on the user's behalf regarding the Node Secret. The Node Secret can be cleared in the NetClarity NACwall by navigating to **System>RSA Configuration**.

sdconf.rec:

The sdconf.rec file will be contained in a zip file when downloaded from your RSA Authentication Manager. The zip file should be uploaded using the NetClarity NACwall menu choice **System>RSA Configuration.**

sdopts.rec:

The sdopts.rec file will be created and stored by the system. No action is required on the user's behalf regarding this file.

sdstatus.12:

The sdstatus.12 file will be created and stored by the system. No action is required on the user's behalf regarding this file. The sdstatus.12 file can be cleared in the NetClarity NACwall by navigating to **System>RSA Configuration**.